Defending Against Probe-Response Attacks

Emmanouil Vasilomanolakis*, Noorulla Sharief†, Max Mühlhäuser*
Telecooperation Lab,
Technische Universität Darmstadt
Darmstadt, Germany
*{vasilomano, max}@tk.tu-darmstadt.de
†noorulla.sharief@stud.tu-darmstadt.de

***Abstract*—With the increase in the sophistication of cyber-attacks, collaborative defensive approaches such as Collaborative IDSs (CIDSs) have emerged. CIDSs utilize a multitude of heterogeneous monitors to create a holistic picture of the monitored network. Nowadays, a number of research institutes and companies deploy CIDSs that publish their alert data publicly, over the Internet. Such systems are important for researchers and security administrators as they provide a source of real-world alert data for experimentation. However, a class of attacks exist, called Probe-Response Attacks (PRAs), which can significantly reduce the benefits of a CIDS. In particular, such attacks allow an adversary to detect the network location of the monitors of a CIDS.**

In this paper, we first study the related work and analyze the various mitigation techniques for defending against PRAs. Subsequently, we propose a novel mitigation mechanism that improves the state of the art. Our method, namely the Shuffle-based PRA Mitigation (SPM), is based on the idea of shuffling the watermarks, so-called markers, which the adversary requires to successfully perform a PRA. By doing so the whole process of the attack is disrupted leading to a very small number of identified monitors. Our experimental results suggest that our proposed method significantly reduces the impact of a PRA whilst it does not introduce a trade-off for the usability of the data produced by the CIDS.

I. Introduction

Sophisticated and highly tailored attacks, e.g., Distributed Denial of Service (DDoS) attacks and Advanced Persistent Threats (APTs), are constantly increasing [14]. To cope with this, research in cyber-security is moving from isolated security solutions such as honeypots and Intrusion Detection Systems (IDSs) [10] towards more collaborative approaches [20]. Such systems, called Collaborative IDSs (CIDSs), function by making use of a plethora of monitors, which collaborate by exchanging alert data, to create a holistic view of the monitored network [17].

Over the years a number of research institutes and corporations have deployed CIDSs which publish their alert data publicly over the Internet. For instance, the DShield [15] and TraCINg [16] CIDSs belong into this category. In more details, a glance of such an example of publicly available alert data, in the TraCINg[1] CIDS (developed by us in our previous work [16]), is given in Figure 1.

[1]http://www.tracingmonitor.org

These systems, also referred to as cyber incident monitors or network telescopes, are important for both the research community and for securing the Internet in general. For instance, DShield aided in the early detection of the Code-Red worm [11]. In addition, such publicly available alert data can assist researchers for their experiments. For instance, alert datasets are very important for the evaluation of intrusion detection algorithms and systems.

A lot of research has been conducted with regard to CIDSs and potential attacks [6]. In particular, a class of *disclosure* attacks exists that makes it possible for an adversary to identify the network location, i.e., the IP address, of the monitors of a CIDS. These attacks are called Probe-Response Attacks (PRAs) and can have a significantly negative impact for a CIDS. For example, an attacker can utilize such knowledge to either attack the CIDS monitors, e.g., via DDoS attacks, or to create sophisticated malware that are able to evade monitors and thus remain undetected for a longer period of time.

In our previous work we have introduced an open-source framework for the deployment, experimentation and mitigation of PRAs [18]. Moreover, we have shown that the impact of such attacks is high and that PRAs can be realistically deployed even from an attacker with low bandwidth capabilities [19]. Lastly, we proposed a method for the detection of a PRA based on certain statistical properties as well as a mitigation mechanism that performs adaptive reporting via sampling the alert data output of the CIDS.

In this paper, we propose a mitigation technique that attempts to significantly decrease the accuracy of a PRA while introducing minimal changes to the (publicly available) alert data output of the CIDS. More specifically, the approach presented here, called Shuffle-based PRA Mitigation (SPM), is based on shuffling the various outputs of the CIDS that can act as watermarks and thus utilized by an adversary. In contrast to the related work our approach neither reduces the output of the CIDS nor contaminates the output of the system (making it unusable). We evaluated our proposal in a simulation framework, with real-world data from the DShield CIDS, and the experimental results suggest that the shuffling mechanism is highly effective against PRAs.

The remainder of this paper is organized as follows. In Section II, we provide background information for PRAs by thoroughly discussing how the attacks operate. Moreover,

Attack Type	Date	Source Country	Source City	Source Port	Destination Country	Destination City	Destination Port
Portscan	2017-01-03 05:17	Turkey	Üsküdar	19506	Greece	Athens	6789
Portscan	2017-01-03 12:02	Turkey	Üsküdar	45182	Greece	Athens	23
Portscan	2016-12-31 01:31	China	Ürümqi	27636	Greece	Athens	23

Fig. 1: Publicly available alert data output in the TraCINg CIDS

Section III, discusses the related work with an emphasis on existing detection and mitigation techniques. Furthermore, Section IV proposes and discusses our mitigation method. It also compares this approach, via a qualitative comparison, with all existing mitigation techniques. Subsequently, Section V presents the results of our simulation experiments. Finally, Section VI concludes this paper and suggests ideas for future work.

II. Background

CIDSs can be classified, with respect to their network architecture, into centralized, hierarchical and distributed [17]. Each of these classes has its own advantages with regard to the scalability and the overall accuracy of the CIDS. Regardless of the utilized architecture it is important, for all CIDSs, that the monitors that exchange alert data remain *anonymous*.

PRAs are a special class of disclosure attacks that target CIDSs which publish their alert data publicly over the Internet. Even though the majority of such systems, which lie in this category, exhibit a centralized architecture, e.g., [15], [16], the applicability of the PRAs is agnostic to the architecture of the CIDS [13]. The only requirement is the ability to access the alerts generated by the CIDS. This is usually achieved by either a web front-end (e.g., similar to Figure 1) or via the utilization of an Application Programming Interface (API).

PRAs were introduced by Lincoln et al. [8] and were further analyzed by several researchers, e.g., [1], [2], [12], [13]. In the following, a summary of the idea of the PRA is given along with a brief description of the improvement mechanisms that we proposed in [19]. An overview of the lifecycle of such an attack is given in Figure 2.

The attack involves several steps, which can be summarized in the following. The adversary starts a PRA by dividing the whole IPv4 address space into equally sized groups (for the sake of simplicity, Figure 2, initially assumes a total of six hosts divided into two groups). Each group is assigned a distinct specially crafted watermark, also known as *marker*. This implies that every host inside a group will be tagged with the same marker. A marker can take many forms; for instance, the adversary can use an uncommon source port to afterwards distinguish the marker from the responses received from the CIDS.

Subsequently, the attacker will probe each host with the respective marker. If a monitor is present among the probed hosts, it will classify the probe as an attack and notify the corresponding CIDS server. The CIDS will publish this incident in its publicly available report. By inspecting the

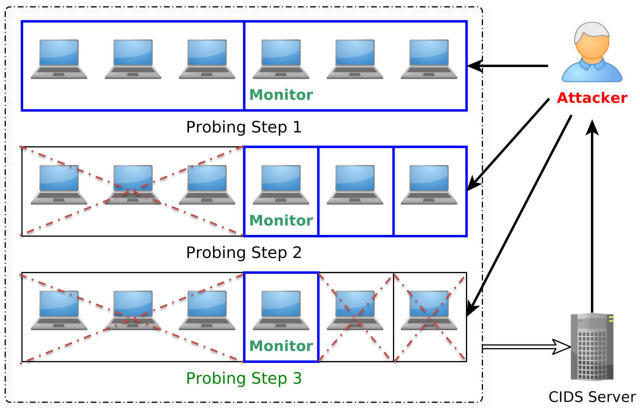

Fig. 2: Probe-Response Attack (PRA) lifecycle overview [18]

CIDS's published reports, the attacker can determine to which group the monitor belongs to (by examining the respective marker). Afterwards, the adversary carries on with the attack by sending a large number of probes in the respective address space.

At a glance, the driving idea behind such a *divide and conquer* attack is that the markers can be subsequently utilized for examining the output of the CIDS and determining whether it contains signs of the markers or not. In this context, and with respect to the received output from the CIDS, the attacker can reduce the probed IP space and repeat the probing steps until the monitors' addresses are revealed.

Bethencourt et al. presented a PRA that follows the aforementioned logic, along with algorithms for efficient probing [2]. In addition, the authors described a variety of adversarial models with regard to the capabilities of the attacker, e.g., the available bandwidth. Bethencourt et al. provided results of various simulations that demonstrate that their PRAs are feasible within a relatively short time-frame. The trade-off, however, is the bandwidth. On the one hand, with a network speed of 384Mbits/s, 3 days are required to conduct a complete PRA. On the other hand, with a network speed of 1.544Mbits/s, 34 days are required.

For PRAs to be practically realized, there is a need for efficient and rapid Internet-wide probing. The assumption behind such attacks is that a CIDS utilizes a large number of reachable monitors that are distributed all over the IPv4 address space. Over the last years, research in this domain has made important improvements, e.g., [4], [9]. In particular,

Durumeric et al. [4] presented ZMap, a tool for performing Internet-wide network scanning. ZMap significantly reduces the required time for an Internet-wide probing, under certain assumptions, to one hour or less.

In our previous work [18], [19], we made significant improvements to the speed of the attacks by utilizing such state-of-the-art techniques in Internet-wide probing and by improving the PRAs themselves. In particular we proposed a generic marker encoding methodology that combines all available *marker* values and introduces the concept of *checksums*. Checksums solve the problem of noise, i.e., attacks that appear in a CIDS and are mistakenly interpreted (by the adversary) as part of the PRA. This is achieved by introducing a small checksum field inside the marker; eventually, when the attacker examines the CIDS output, to be considered part of the PRA, all markers need to comply with the pre-computed checksum. This mechanism can be implemented with various ways, including checksum algorithms or even symmetric encryption mechanisms. For instance, in [19] we utilized the Fletcher checksum algorithm [5]. The proposed methodology offers two major advantages. First, via the utilization of checksums the adversary can reduce the number of repetitions of the PRA and thus reduce the overall execution time. Second, the checksum approach efficiently deals with noise, a problem that had not been efficiently tackled in related work. Our results, in real-world CIDSs, showed that PRAs can be practically executed in less than a day.

III. Related Work

The previous section provided the background information on PRAs. In this section, all the prominent proposed mitigation techniques that have been identified in the related work are discussed. Note that the mitigation mechanisms that are described in this section assume a method for the detection of a PRA. For this, the reader can refer to our previous work [19].

A. Hashing and Encryption

As the name implies *hashing*, in the context of PRA mitigation, refers to the process of utilizing a hash function (or a cryptographic approach) to map marker values. By doing so, the respective parameters become unusable from the adversaries' perspective, thus reducing the applicability of the PRA. This defense mechanism was first proposed by Bethencourt et al. [2]. An example of the utilization of the hashing mechanism is shown in the second column of Figure 3. Specifically, in this example the destination port values have been hashed via the utilization of the MD5 hash function. A similar approach is *encryption*; here instead of utilizing a hash function the defender can instead encrypt a parameter either symmetrically or asymmetrically.

There are a number of shortcomings with regard to hashing. First, hashing seriously damages the usability of the dataset making it unreadable for the legitimate users. Furthermore, in the case in which the mitigation mechanism is activated only upon detection of a PRA, the adversary will immediately realize that the attack has been identified. Similarly, a malicious entity may choose to utilize such knowledge to enforce the CIDS to perform hashing and thus reduce its usability. Lastly, when a known hash function (instead of an encryption scheme such as symmetric encryption) is utilized for a specific range of integer values (e.g., port numbers) an attacker may use a rainbow-table like technique to create a database of all possible values. Correspondingly the adversary can reverse the hash values. Encrypting the markers can assist for some of the aforementioned disadvantages but does not offer a solution for the usability trade-off.

B. Adaptive Sampling

Sampling was first mentioned in [2] and was further improved and analyzed in our previous work [18], [19]. In more details, the idea behind this mitigation method is that the CIDS will selectively publish only a sample of the overall generated attacks whenever it detects the presence of a PRA. The intensity of the sampling can also be proportional to the attack intensity [19]. Therefore, the attacker will not be able to retrieve all the marker probes from the CIDS, which leads to a reduction of the effectiveness of the attack. Our simulation results suggested that, by utilizing this adaptive sampling approach, only the 31% of the total monitors were detected by the PRA [19]. However, as a result of the sampling process, there is also a reduction of 62% in the total number of events that are reported by the CIDS.

The main shortcoming of sampling is the impact that it has in the usability of the CIDS. That is, the system publishes only a small portion of the overall alert data. In fact, an adversary might attempt to exploit this mechanism and perform a type of a Denial of Service (DoS) attack on the system. Moreover, the trade-off between effectiveness and usability is not very satisfying as a 31% PRA success rate is rather high.

C. Other approaches

There have been proposed some additional approaches for the mitigation of PRAs that, however, require either a dramatic reduction of the usability of the system or an overwhelming overhead for the administrators. Hence, the approaches, that are briefly described in the following, are considered out of the scope of this paper and thus will not be further discussed.

First, a naive approach for completely canceling the ability to perform a PRA is by cutting out the feedback loop. This can be easily done by making the CIDS private, e.g., by enforcing access control into its contents [2]. Nevertheless, such an approach completely disregards the benefits of sharing alert data publicly. Second, another approach is to regularly change the network position, i.e., the IP address, of the monitors [2]. Such an approach would effectively tackle the PRA problem but it would also introduce massive overhead for the administrators of the system. For instance, in the DShield CIDS there are approximately $500,000$ monitors, which, in their majority, are managed by organizations outside DShield. Furthermore, in many organizations the range of IP address (especially with regard to IPv4) is very limited. Finally, another method is

Source IP Address	Source Port	Destination Port (Hashed)	Protocol	Flag	Sensor ID
187.037.016.067	7874	b6d767d2f8ed5d21a44b0e5886680cb9	6	S	*C7193249F12F2901483A4A7EDC2D114CD82DA379
062.176.090.066	53714	197838c579c3b78927e0cd15ba4c9689	6	S	*C7193249F12F2901483A4A7EDC2D114CD82DA379
183.033.018.178	8491	9087cd8bfa9c1968b20d8f6d0b81cbbb	6	S	*8E0A3567342156094C7843E203AA4F51269A6E99

Fig. 3: Example of hashing the destination port marker in the DShield data

the addition of *noise* data in the CIDS output. Based on the specifics of the noise data this approach can mitigate the original PRA [2]. However, such an approach cannot defend against the more sophisticated PRAs [19] due to the watermark that is included inside the markers. In addition, this method contaminates the alert data.

IV. Shuffling-based PRA Mitigation

On the basis of the shortcomings of the state of the art, this section proposes a novel method for the mitigation of PRAs.

The idea behind our proposal is based on the fact that only a few of the parameters in the publicly available output of CIDS can be actually utilized as probe markers [18]. These possible markers can be easily anticipated by carefully examining the CIDS. For instance, Figure 1 depicts all the output parameters of the TraCINg CIDS from which one can derive all possible probe markers (e.g., the destination port).

Based on this observation we propose the Shuffle-based PRA Mitigation (SPM). In SPM the defender shuffles, i.e., changes the positions, of certain parameters upon detection of a PRA. This concept is inspired by the *shell game*, a deception approach that has also been used as a state of the art technique for achieving anonymity [3]. With our technique we attempt to bridge the trade-off between effectively defending against PRAs and, by doing so, reducing the usability of the CIDS.

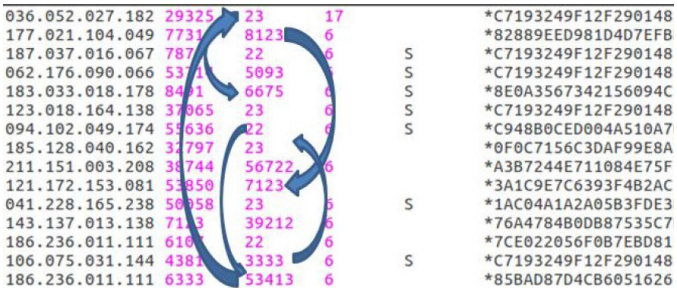

Fig. 4: Example of the shuffling procedure in DShield data

The shuffling in SPM is stochastic and can be realized via the utilization of a pseudo-random function. As expected, due to the stochastic nature of the process and the limited range of the parameters (e.g., ports can have 65537 possible values) there will be cases in which the result of the shuffling process will be the same with the original parameter. However, as it will be shown in the next section (see Section V-B), only a very small portion of the monitors can be detected as result of this. Figure 4, illustrates an example of the SPM procedure in the case of DShield data when adjusting the destination port value. Note that for the sake of visual clarity the figure depicts the shuffling process only for some of the parameters.

The main advantage of the SPM approach is that it requires minimal modifications in the alert data. Note that as the data is shuffled, but not altered, global statistics will still be valid (e.g., creating lists of most commonly attacked ports or protocols). Moreover, the adversary cannot know if the CIDS has detected the presence of the PRA and/or whether the system has activated defense measures. This is not the case with other methods such as the hashing and the encryption of the alert data. In addition, as it will be shown in the next section SPM is highly effective (see Section V-B). Finally, it is possible to utilize pseudo-random generators of which the utilized seeds can be shared with trusted users so that the whole process can be reversible. Note that, this does not influence the effectiveness or the security of the mechanism (against the PRA) since the adversary cannot predict whether the SPM is activated in a certain time-window or not.

We argue that there is a trade-off between defending against a PRA and maintaining the usability of the CIDS. Therefore, the respective research challenge is to identify mechanisms that, on the one hand, disrupt the PRA process while, on the other hand, introduce minimal or zero overhead on the operation of the system. The proposed SPM mechanism is a step towards such a task.

Table I, brings together the analysis of the previous section with the mitigation mechanism presented here. In particular, it compares the different mitigation mechanisms presented in Section III and the SPM with regard to the PRA defense level and the overall CIDS usability level (after the implementation of the respective measure). The comparison here is *qualitative* and follows the argumentation of the paper. Nevertheless, the findings of Table I, and specifically with regard to the PRA defense level, correspond to the simulation results as shown in the following section. Measuring the usability level of a CIDS, while deploying PRA defense mechanisms, in an unbiased manner is a challenging task and is considered out of the scope of this paper.

Mitigation Technique	PRA Defense Level	CIDS Usability Level
None	○○○○○	●●●●●
Non-public CIDS	●●●●●	○○○○○
Hashing or Encryption	●●●●●	●○○○○
Sampling	●●○○○	●●●○○
Noise	●○○○○	●●○○○
SPM	●●●●○	●●●●○

TABLE I: Comparison of different PRA mitigation techniques: "○ ○ ○ ○ ○" indicates the lowest (worst-case) possible value, while "● ● ● ● ●" the highest (best-case) one

V. Evaluation

This section presents the evaluation and comparison of our proposed SPM mechanism with the state of the art.

A. Simulation Setup

For the evaluation of the proposed mitigation mechanism, we have setup a simulation environment that is similar and comparable to our previous work [19]. In particular, our simulation follows the characteristics of DShield [15]. DShield is one of the largest and most well known CIDSs, reporting thousands of potential attacks. Along with the DShield characteristics, we also take into consideration previous work in the area of Internet-wide scanning as our methodology relies on scanning the entire range of IP addresses exposed on the Internet.

All the simulations use the following parameters. We utilize a set of approximately 288.4 million responsive IPv4 addresses, as identified in the related work [7], [9]. Within all these responsive addresses, we set a total of 500 thousand monitors randomly. This follows the number of monitors that DShield is utilizing [15]. In addition, as network traffic does not always reach its destination, we also take into account a 2% packet *drop rate*. This drop rate has been observed in previous work from [4], [7]. Lastly, the simulation utilizes a low *bandwidth* of $56Mbit/s$, so as to support the potential bandwidth capabilities of a large number of adversaries.

B. Simulation Results

In the following we provide and discuss the simulation results in the following order. First, we examine how SPM performs in general and compare the results with the case of a CIDS that does not employ any defense mechanism. Subsequently, we compare the SPM to the two most prominent defense techniques: *hashing* and *sampling*.

Figure 5, depicts a comparison of the SPM technique compared to a CIDS without any mitigation mechanism. Note that in this case the number of identified monitors is, in some cases, larger than $500,000$ as a result of false positives (when no checksum or low checksum values are chosen)[2]. Overall, the attacker can detect all the monitors of the CIDS, without false positives, by utilizing a combination of 24 marker bits and 8 bits for the checksum. Moreover, note that the y-axis uses a logarithmic scale to be able to depict the large amount of identified monitors.

On the contrary, when the SPM process is activated the number of detected monitors drops from $500,000$ (i.e., all monitors) to approximately 100. This translates to a reduction of 99.98% to the number of (correctly) identified monitors and hence can be considered highly effective. Moreover, Figure 5 also shows that shuffling is independent of the checksum bit size that the adversary may utilize.

Figure 6, compares hashing to our shuffling approach. As expected hashing is superior in the sense that it can completely stop the PRA. This is the result of hashing the probe markers and therefore making them unusable for the adversary. Note that, in our experiments, we assume that the hashing technique has been applied to the CIDS parameters that are chosen as markers by the attacker (in this example case hashing was applied to the *destination port* parameter).

[2]For further details on the false positive (noise) problem and the PRAs the reader can refer to our previous work [19].

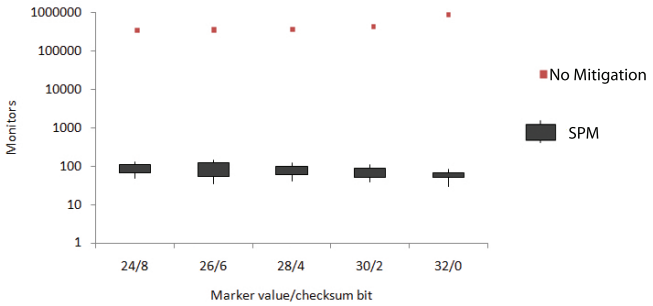

Fig. 5: PRA-identified monitors with shuffling (SPM) and without any countermeasure

As discussed in the previous sections, hashing (and similarly encryption) can be an efficient solution for the mitigation of PRAs. Nevertheless, this comes with a trade-off between the usability of the CIDS data and the accuracy of the PRA. As it was discussed in the previous section (cf. Table I and Figure 3) hashing severely degrades the usability of the system.

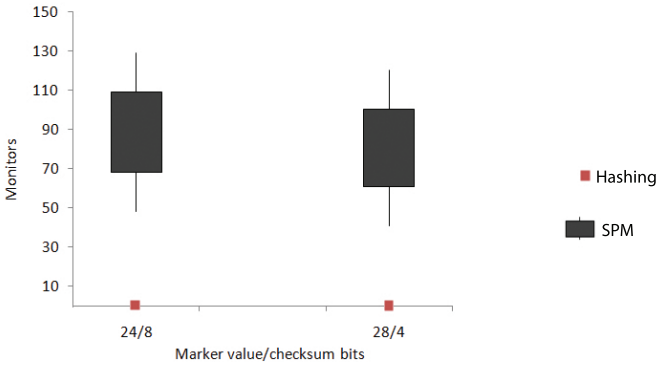

Fig. 6: Comparison of the shuffling (SPM) mitigation technique and hashing

Lastly, Figure 7 compares the SPM to sampling. Note that similarly to Figure 5, the y-axis uses a logarithmic scale. In our previous work [19], we have shown that sampling can reduce the effectiveness of the PRA by around 70%. However, this implies that around $150,000$ monitors can still be identified by the adversary. In addition, the usability of the system is reduced as a result of the sampling process. On the contrary the SPM significantly reduces the number of identified monitors compared to sampling, and requires minimal changes to the alert data output.

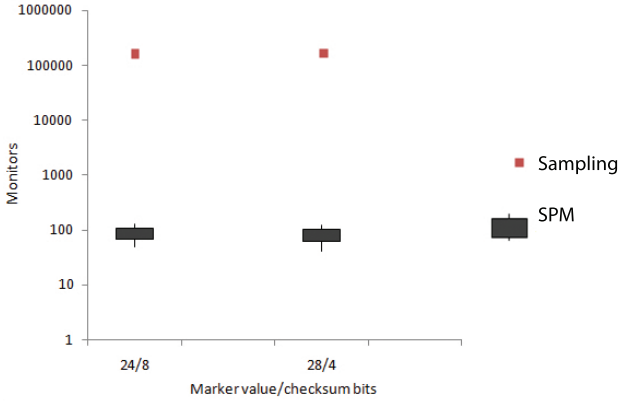

Fig. 7: Comparison of the shuffling (SPM) mitigation technique and sampling

VI. Conclusion

Probe-Response Attacks (PRAs) introduce a threat to a Collaborative IDS (CIDS) by allowing to malicious entities to detect the network location (IP addresses) of the monitors of the system. Defending against such attacks is not an easy task and by examining the related work a trade-off was identified between successful mitigation and the usability of the CIDS's output after the implementation of the defensive measures. We present a method, namely Shuffle-based PRA Mitigation (SPM), for defending against PRAs that is based on shuffling the parameters in the CIDS's output that can act as a PRA marker. Our experimental results suggest that the proposed shuffling mechanism improves the state of the art as it significantly reduces the accuracy of the PRA with a minimal modification of the output of the system; thus maintaining its usability.

With regard to future work we aim on further improving our shuffling technique with respect to the usability of the CIDS's output data. For instance, we envision the utilization of certain pseudo-random generators, for the shuffling process, for which the utilized seeds can be shared with trusted users making the process reversible.

VII. Acknowledgments

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Program, PROTECTIVE, under Grant Agreement No 700071.

References

[1] Paul Barford, Somesh Jha, and Vinod Yegneswaran. Fusion and filtering in distributed intrusion detection systems. In *Proc. Allerton Conference on Communication, Control and Computing*, 2004.

[2] John Bethencourt, Jason Franklin, and Mary Vernon. Mapping internet sensors with probe response attacks. In *USENIX Security Symposium*, pages 193–208, 2005.

[3] Jörg Daubert, Mathias Fischer, Tim Grube, Stefan Schiffner, Panayotis Kikiras, and Max Mühlhäuser. Anonpubsub: Anonymous publish-subscribe overlays. *Computer Communications*, 76:42–53, 2016.

[4] Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. ZMap: Fast Internet-wide Scanning and Its Security Applications. In *Proceedings of the 22nd USENIX Security Symposium*, pages 605–619, 2013.

[5] John G Fletcher. Arithmetic checksum for serial transmissions. *IEEE Transactions on Communications*, (1):247–252, 1982.

[6] Carol Fung. Collaborative intrusion detection networks and insider attacks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 2(1):63–74, 2011.

[7] John Heidemann, Yuri Pradkin, Ramesh Govindan, Christos Papadopoulos, Genevieve Bartlett, and Joseph Bannister. Census and Survey of the Visible Internet. In *Proceedings of the ACM Internet Measurement Conference*, pages 169–182, 2008.

[8] Patrick Lincoln, Phillip A. Porras, and Vitaly Shmatikov. Privacy-preserving sharing and correction of security alerts. In *13th USENIX Security Symposium*, pages 239–254, 2004.

[9] Dirk Maan, José Jair Santanna, Anna Sperotto, and Pieter-tjerk De Boer. Towards validation of the Internet Census 2012. In *20th EUNICE/IFIP EG 6.2, 6.6 International Workshop*, pages 85–96. Springer, 2014.

[10] Robert Mitchell and Ing-Ray Chen. A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys (CSUR)*, 46(4):55, 2014.

[11] David Moore, Colleen Shannon, and Jeffery Brown. Code-Red: A Case Study on the Spread and Victims of an Internet Worm. In *Second ACM SIGCOMM Workshop on Internet Measurment (IMW)*, pages 273–284, 2002.

[12] Yoichi Shinoda, Ko Ikai, and Motomu Itoh. Vulnerabilities of passive internet threat monitors. In *USENIX Security Symposium*, pages 209–224, 2005.

[13] Vitaly Shmatikov and Ming-Hsiu Wang. Security against probe-response attacks in collaborative intrusion detection. In *Workshop on Large scale attack defense - LSAD*, pages 129–136, New York, USA, 2007. ACM.

[14] Aditya K. Sood and Richard J. Enbody. Targeted Cyber Attacks-A Superset of Advanced Persistent Threats. *IEEE Security & Privacy*, 11(1):54–61, 2013.

[15] Johannes Ullrich. Dshield internet storm center. https://www.dshield.org/, 2000.

[16] Emmanouil Vasilomanolakis, Shankar Karuppayah, Panayotis Kikiras, and Max Mühlhäuser. A honeypot-driven cyber incident monitor: lessons learned and steps ahead. In *International Conference on Security of Information and Networks*, pages 158–164. ACM, 2015.

[17] Emmanouil Vasilomanolakis, Shankar Karuppayah, Max Mühlhäuser, and Mathias Fischer. Taxonomy and Survey of Collaborative Intrusion Detection. *ACM Computing Surveys*, 47(4):33, 2015.

[18] Emmanouil Vasilomanolakis, Michael Stahn, Carlos Garcia Cordero, and Muhlhauser Max. Probe-response attacks on collaborative intrusion detection systems: Effectiveness and countermeasures. In *Communications and Network Security (CNS)*, pages 699–700. IEEE, 2015.

[19] Emmanouil Vasilomanolakis, Michael Stahn, Carlos Garcia Cordero, and Max Mühlhäuser. On probe-response attacks in collaborative intrusion detection systems. In *Conference on Communications and Network Security (CNS). IEEE*, 2016.

[20] Chenfeng Vincent Zhou, Christopher Leckie, and Shanika Karunasekera. A Survey of Coordinated Attacks and Collaborative Intrusion Detection. *Computers & Security*, 29(1):124–140, feb 2010.